FortiClient v5.0 Patch Release 7
Upgrade Guide

FortiClient v5.0 Patch Release 7 Upgrade Guide

December 13, 2013

04-500-225408-20131213

Technical Documentation	docs.fortinet.com
Knowledge Base	kb.fortinet.com
Customer Service & Support	support.fortinet.com
Training Services	training.fortinet.com
FortiGuard	fortiguard.com
Document Feedback	techdocs@fortinet.com

Table of Contents

Change Log

Date	Change Description
2013-12-13	Initial Release.

Introduction

FortiClient v5.0 Patch Release 7 supports upgrade from FortiClient v4.0 MR2. There are three ways to complete an upgrade:

- manually,
- through the FortiGuard Distribution Server (FDS), or
- through a FortiManager device.

Corporate users with a large installation of FortiClient v4.0 MR2 clients, that are managed by FortiManager are encouraged to use the third option.

FortiClient v5.0 does not support the use of FortiManager for central management. FortiGate devices running FortiOS v5.0 may be used for endpoint control.

After a successful upgrade, previously managed FortiClient systems will no longer be managed by FortiManager. The administrator should consider the impact of this on FortiClient distribution.

A successful software upgrade will convert and update all existing FortiClient v4.0 MR2 configurations to FortiClient v5.0 Patch Release 7 formats. For information on exceptions, see the Known Issues section in the *FortiClient Release Notes* before starting an upgrade.

An Internet connection is required for both manual and FDS software upgrades.

For information about the new features in FortiClient v5.0 Patch Release 7, please see the *FortiClient Administration Guide*, available from the Fortinet Technical Documentation website.

Feature differences

FortiClient v4.0 MR2 comes in the following different versions:

- FortiClient full version

  Includes AntiVirus, IPsec VPN, Network Layer Firewall, Web Filtering, and AntiSpam
- FortiClient IPsec VPN Lite
- FortiClient SSL VPN standalone

FortiClient v5.0 differs as follows:

- There is only one installer type, with two options: 32 bit or 64 bit
- The following features have been removed:
  - Network Layer Firewall
  - AntiSpam
- In the FortiClient console, the following features were merged:
  - IPsec VPN
  - SSL VPN standalone

The SSL VPN standalone installer is still available, but is no longer offered as a separate installation.

- The IPsec VPN Lite installer no longer exists

It is still possible to install VPN only using v5.0.

Upgrade

This chapter explains upgrading FortiClient v4.0 MR2 to v5.0 Patch Release 7 manually and through the FDS.

Manual upgrade

FortiClient v4.0 MR2 may be upgraded to FortiClient v5.0 Patch Release 7 by running the FortiClient v5.0 Patch Release 7 installation file on the client computer. The installation file can be downloaded from the following locations:

- Fortinet Customer Service & Support: https://support.fortinet.com

  This requires a support account with a valid support contract.
- FortiClient homepage: www.forticlient.com

  The installer file performs a virus and malware scan of the target system prior to installing FortiClient if antivirus software is not detected.
- Fortinet Resource Center: http://www.fortinet.com/resource_center/product_downloads.html

  Download the FortiClient online installation file.
- The FortiGate dashboard

  In FortiOS v5.0 Patch Release 1 or later, you can download the FortiClient installation files in the FortiGate dashboard. Go to *System* > *Dashboard* > *Status*, in the *License Information* widget select Mac or Windows to download the FortiClient Online Installer.

See the *FortiClient Administration Guide*, available from http://docs.fortinet.com/fclnt.html, for more information.

Upgrade through FDS

FortiClient v5.0 Patch Release 7 is available through the FDS to existing FortiClient v4.0 MR2 users. Existing users will have received an update notification that they may choose to accept or reject.

If the user accepts the update, the installation of FortiClient v5.0 Patch Release 7 will proceed. If the update notice is rejected, the notification may be repeated at regular intervals. The upgrade can be postponed indefinitely, and FDS notifications disabled, by selecting *Never ask me again*.

Some users may have configured FortiClient to run updates automatically. For these users, the upgrade will proceed without a prompt.

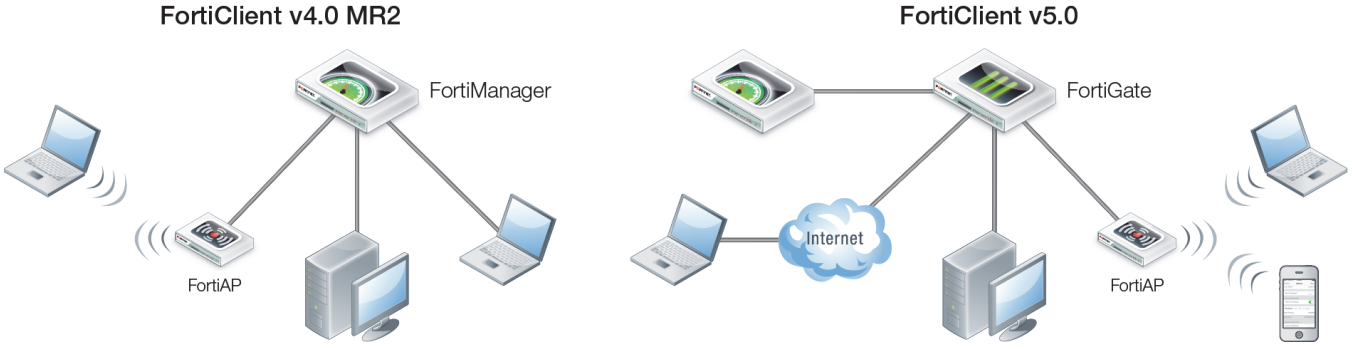
Upgrade through FortiManager

This chapter explains upgrading FortiClient v4.0 MR2 to v5.0 Patch Release 7 through FortiManager.

Compared with FortiClient v4.0 MR2, the v5.0 client registers with, and receives configuration updates from, the local FortiGate unit or units in the network, see Figure 1. The FortiManager device is used to manage the FortiGate units, and to centrally manage the endpoint profiles and assignments across all devices in the network. FortiManager can also be used for central logging and reporting, and local security services (AV, IPS, Web Filtering, etc).

A client can be connected directly to a FortiGate device, either to a physical port, a switch, or over WiFi. A client can also be connected from behind a router or NAT device, or across a VPN connection.

Figure 1: FortiClient network topologies



FortiClient v4.0 MR2 client computers that are managed by FortiManager may be upgraded to FortiClient v5.0 Patch Release 7 by pushing the update from the FortiManager.

A software upgrade may be initiated by the administrator by manually uploading the FortiClient v5.0 Patch Release 7 MSI installation package to FortiManager v4.0 MR3.

The end-user receives a notification requesting permission to proceed with the upgrade. The manual package upload allows the administrator to configure the IP address of a FortiGate that will manage the clients upon completion of the upgrade.

The following steps are discussed in this chapter:

- Configure endpoint control on the FortiGate
- Customized FortiClient 5.0 installer
- Distribute the installer from the FortiManager

When a large deployment of FortiClient v4.0 MR2 users is involved, the administrator can execute this procedure in a test lab before deploying to production.

Configure endpoint control on the FortiGate

The following endpoint control capabilities will be useful to existing administrators of managed FortiClient v4.0 MR2 users:

- Silent registration
- Locked FortiClient settings
- Disable unregister
- Monitoring registered users
- Using Active Directory groups
- Multiple redundant FortiGates

Configuration of endpoint control is discussed in detail in the *FortiClient Administration Guide*. XML syntax is defined in the *FortiClient XML Reference* (see http://docs.fortinet.com/fclnt.html). Examples of each of the capabilities above are provided here. A sample configuration file is shown in "Putting it together" on page 11.

Silent registration

Following a successful upgrade of FortiClient v4.0 MR2 to v5.0 Patch Release 7, the end user does not need to be prompted to register to a FortiGate. The following XML element can be used to enable this:

```
<forticlient_configuration>
  <endpoint_control>
    <silent_registration>1</silent_registration>
  </endpoint_control>
</forticlient_configuration>
```

Locked FortiClient settings

End-users with administrator permission on their Windows system have access to the FortiClient settings page. If this is not desired, it can be locked with a password from the FortiGate. The following FortiOS Command Line Interface (CLI) script, when included, requires any client registered to the FortiGate to provide the password before they can access the settings page.

```
config endpoint-control profile
  edit "fmgr"
    config forticlient-winmac-settings
      ...
      set forticlient-settings-lock enable
      set forticlient-settings-lock-passwd <password>
      ...
      end
  end
```

Disable unregister

With silent endpoint control registration enabled, a user could unregister after FortiClient has registered to the FortiGate. The capability to unregister can be disabled using the following XML element:

```
<forticlient_configuration>
  <endpoint_control>
    <disable_unregister>1</disable_unregister>
  </endpoint_control>
</forticlient_configuration>
```

Monitoring registered users

An administrator can monitor managed FortiClient v4.0 MR2 users on FortiManager before upgrading them to v5.0 Patch Release 7. Following the upgrade, if the client successfully registers to the FortiGate, the client can be monitored on the FortiGate.

In the FortiOS Web-based Manager, all registered clients can be observed on the *User & Device* > *Monitor* > *FortiClient* page. Either of the following FortiOS CLI commands will list all registered clients:

- `diagnose endpoint registration list`, or
- `diagnose endpoint record-list`.

Using Active Directory groups

Some organizations may choose to deploy different endpoint control profiles to different user groups. FortiOS is able to send different endpoint control profiles based on the AD group of the user. This requires use of the FortiAuthenticator.

No special configuration is required on FortiClient. FortiOS configuration details are discussed in the *FortiClient Administration Guide* (see http://docs.fortinet.com/fclnt.html).

Multiple redundant FortiGates

Administrators who have more than one FortiGate serving potential FortiClient users may consider configuring multiple FortiGates for endpoint control registration of clients.

The *FortiClient Administration Guide* describes the FortiOS and FortiClient configurations required to enable this feature.

Putting it together

Here is a sample complete FortiClient v5.0 Patch Release 7 XML configuration file with the aforementioned capabilities:

```
<forticlient_configuration>
  <partial_configuration>1</partial_configuration>
  <endpoint_control>
    <enabled>1</enabled>
    <disable_unregister>1</disable_unregister>
    <silent_registration>1</silent_registration>
    <fortigates>
      <fortigate>
        <serial_number />
        <name />
        <registration_password>un9r3Ak@b!e</registration_password>
        <addresses>newyork.example.com</addresses>
      </fortigate>
    </fortigates>
  </endpoint_control>
</forticlient_configuration>
```

The FortiGate that the FortiClient is registered to is listed in the `<fortigates>` element. The `<registration_password>` element is required if the endpoint control configuration on the FortiOS requires one. This can be provided in plain text or as an encrypted file.

The configuration provided above is not the full FortiClient configuration file. Thus, the `<partial_configuration>` element is set to 1.

Customized FortiClient 5.0 installer

The publicly available FortiClient v5.0 installer can be used to upgrade standalone (not managed by FortiManager) FortiClient v4.0 MR2 clients. After the upgrade is done, the new FortiClient v5.0 will not register to any FortiGate devices. Manual intervention is required.

An administrator could prepare a custom XML configuration file that requires FortiClient v5.0 Patch Release 7 to register using endpoint control to a FortiGate. This customized configuration can be embedded into the FortiClient installer using the FortiClient Configurator tool, see the *FortiClient Administration Guide* at http://docs.fortinet.com/fclnt.html for more information.

Distribute the installer from the FortiManager

Before distributing the installer from a FortiManager device, verify that the customized FortiClient v5.0 Patch Release 7 installer works correctly. After verifying its function, upload the installer to the FortiManager device, then distribute it to managed clients.

Monitor the status of the clients on the FortiManager unit and on the FortiGate devices to which the clients have been configured to register. FortiClient will register to the FortiGate device after the upgrade.

Push update from FortiManager to managed FortiClient agents:

1. Obtain the FortiClient v5.0 Patch Release 7 installation files from the Fortinet Customer Service & Support portal, https://support.fortinet.com. To download firmware images you require a support account with a valid support contract.
2. Configure the IP address of the FortiGate that will be used for managing the clients after the upgrade is completed.
3. Create a custom MSI installer file.
4. Configure endpoint control on your FortiGate device.
5. Upload the customized MSI installer file to FortiManager.
6. Distribute the MSI installer file to registered clients.

   FortiClient will register to the FortiGate device after the update.

Index